קריפטוגרפיה

השם "קריפטוגרפיה" מקורו במילה היוונית "קריפטו" (κρυπτός) שמשמעותה נסתר או אמנות ההסתרה, ו"גרפיה" (γράφω) שמשמעותה "כתיבה".

- **סודיות או חשאיות (באנגלית: confidentiality)**

סודיות מושגת על ידי הצפנה שנעשית על ידי השולח באמצעות מפתח הצפנה סודי ובמסגרתה המסר הגלוי מועבר למצב מוצפן ופענוח שנעשה על ידי המקבל ובמסגרתו המסר המוצפן חוזר להיות גלוי. לעיתים מפתח ההצפנה זהה למפתח הפענוח ולעיתים שונה.

בקריפטוגרפיה מודרנית בשני השלבים האמורים משתמשים השולח והמקבל בפרוטוקולים ובאלגוריתמים קריפטוגרפיים להשגת סודיות. כאשר השיטות עצמן אינן סודיות והן ידועות ומוסכמות מראש - רק מפתח ההצפנה סודי.

- **אימות (באנגלית: Authentication)**

במערכת קריפטוגרפית שלמה, סודיות לבדה אינה מספקת. יש צורך בנוסף ב**פרוטוקול אימות זהויות** שנועד למנוע התחזות וכן לספק דרך לדעת מיהו מקור המידע, בדומה לפונקציה שממלאת חתימה על גבי המחאה.

- **הבטחת שלמות (באנגלית: Integrity)**

הבטחת שלמות נעשית בדרך כלל על ידי אלגוריתם אימות שתפקידו להבטיח שהמידע (שאינו בהכרח מוצפן) אותנטי, כלומר שלא נעשה בו שינוי זדוני כלשהו על ידי צד שלישי, אויב או מתחרה.

כל שינוי אפילו קל מאוד יתגלה מיד על ידי המשתתפים הלגיטימיים, מה שיגרום למערכת להיפטר מהמידע הפגום ולשלוח הודעת שגיאה מתאימה.

בס"ד

הצפנה קלאסית

הצפנה ככלי לקידוד והסתרת מידע הייתה קיימת משחר ההיסטוריה. בראשית דרכה הייתה ההצפנה בעיקר אמנות לקסיקוגרפית שנעשתה בשיטות פרימיטיביות ידניות.

שיטות ההצפנה בהן עסקו בעת העתיקה, עד תחילת המאה העשרים, נקראות **הצפנה קלאסית** במובן זה שהן נעשו בשיטת 'נייר ועט' או באמצעים מכניים בסיסיים כמו גליל הצפנה, או בשיטות סטגנוגרפיות. זאת בניגוד לקריפטוגרפיה מודרנית שנעשית באמצעות מחשב.

ממצאים המעידים כי המצרים הקדמונים השתמשו בהצפנה בכתב חרטומים, לערך 3000 שנה לפנה"ס. בתנ"ך ובמקורות יהודיים נוספים קיימות עדויות נוספות להצפנה. לדוגמה, בספר ירמיהו (נכתב בשלהי תקופת בית ראשון, לפני שנת 586 לפנה"ס) נכתב "ומלך ששך ישתה אחריהם" (ירמיהו כה כו), "..אל ישבי לב קמי רוח משחית" (ירמיהו נא א). "ששך" היא "בבל" ו"לב קמי" היא "כשדים" בצופן אתב"ש.

השימוש בהצפנה התרחב בתקופת יוון העתיקה. צבא ספרטה השתמש צופן הזזה פשוט. בצופן זה, כל אות משנה את מיקומה לפי חוק מסוים. צפנים אלו מומשו בין היתר בעזרת גליל הצפנה.

יוליוס קיסר (102 עד 40 לפנה"ס) נהג להשתמש בשיטת הצפנה שנקראת צופן החלפה, בה כל אות נשארת במקומה אך מוחלפת באות שונה לפי חוקיות מסוימת. הצופן בו השתמש יוליוס קיסר נודע לימים כצופן קיסר.

כמו כן נעשה בתקופה זו שימוש רב בשיטות סטגנוגרפיות, כגון קעקוע המסר על ראשו המגולח של חייל ושליחתו ליעד לאחר שצמחו שערותיו, או כתיבת המסר על לוחות עץ וציפויים בשעווה לאחר מכן.

דוגמאות מההיסטוריה לשימוש בהצפנה:

- **מברק צימרמן**: מברק מוצפן שנשלח במהלך מלחמת העולם הראשונה (16 בינואר 1917) על ידי שר החוץ של גרמניה, ארתור צימרמן, לשגריר גרמניה בארצות הברית, ומטרתו ליזום ברית בין גרמניה למקסיקו כנגד מדינות ההסכמה. המברק הוצפן באמצעות ספר צופן שנפל בידי המודיעין הבריטי. פענוח המברק היה בין הגורמים להצטרפות ארצות הברית ללחימה לצד מדינות ההסכמה.
- **פרויקט ונונה** (מסמכי וינונה): פרויקט ביון משותף לארצות הברית ואנגליה, לפענוח מסמכים מוצפנים של ברית המועצות שיורטו במהלך מלחמת העולם השנייה, ופוענחו במשך 40 השנים הבאות. מסמכים אלו היוו מקור מידע חשוב עבור הביון של הגוש המערבי במהלך המלחמה הקרה. פיצוח הצופן נבע מטעות שימוש בצד הסובייטי: הצופן בו נעשה שימוש היה מסוג פנקס חד-פעמי, בו כל מפתח משמש פעם יחידה בלבד. ככל הנראה, עקב רצון לחסוך בכמות המפתחות, או עקב הזמן הארוך הנדרש לייצור מפתחות, נעשה שימוש חוזר בחלק מהפנקס החד-פעמי, דבר שהוביל לפענוח חלקי של המסמכים. כ-3,000 מסמכים שיורטו בין השנים 1942 - 1945 פוענחו באופן חלקי או מלא על ידי כוחות הברית, והחל מ-1948 כלל התשדורות שיורטו הפכו בלתי פציחות.

- **שפת הנאוואחו**: השפה המדוברת על ידי אינדיאנים בני שבט הנאוואחו. ניתן לראות בה צופן פשוט הידוע רק לדוברי השפה וזאת מכמה סיבות:

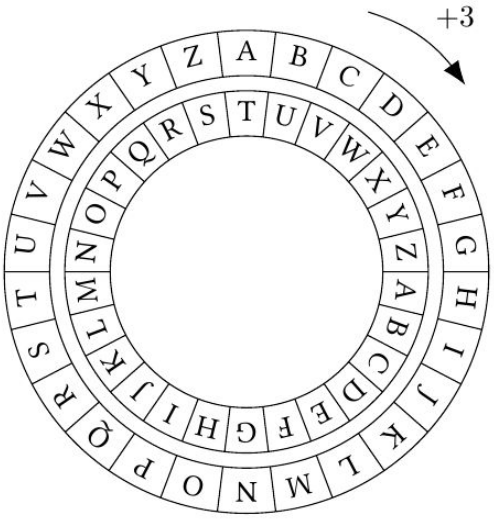
1. בשל מיעוטם היחסי של דוברי השפה והעובדה כי איש מדובריה לא גר בתקופה ההיא בארץ אויב.
2. עקב השונות הגבוהה (יחסית) של שפה זו משפות מודרניות אחרות ושפות נחקרות אחרות, עקב העובדה ששום מוסד לא מלמד שפה זו, הקלטות של השפה היו נדירות ביותר והעובדה כי היא שפה מדוברת בלבד ולא כתובה, קיים קושי רב ב"פיצוח" השפה על ידי בלשנים.

במהלך מלחמת העולם השנייה עשתה ארצות הברית שימוש באלחוטנים בני שבט הנאוואחו להעברת מסרים ברשתות הרדיו, שימוש שהחל עוד בשלהי מלחמת העולם הראשונה לאחר ההבנה שגרמניה בעלת יכולת יירוט של כלל התקשורת הצבאית של ארצות הברית

צופן זה אינו נחשב חזק במיוחד, שכן על מנת לפענחו המודיעין הנגדי צריך להשיג מרגל בן שבט הנאוואחו.

- **אניגמה**: מכונת הצפנה מבוססת רוטור, ששימשה את גרמניה במהלך מלחמת העולם השנייה. בעלות הברית הצליחו לפצח את ההצפנה, ובמשך רוב המלחמה פענחו מספר גדול של הודעות מוצפנות. על מנת שלא לחשוף את העובדה שהמערכת נפרצה על ידי בעלות הברית, נעשה שימוש זהיר ביותר במודיעין שהופק מיירוט מסרים שהוצפנו באניגמה. כמות המידע שהופק מהודעות אלו ואיכותו הובילו את צ'רצ'יל לומר "הודות לאולטרה (המודיעין שהופק מהאניגמה) ניצחנו במלחמה".

צופן קיסר



בתחום הקריפטוגרפיה, **צופן קיסר**, הידוע גם כ**צופן היסט**, **קוד קיסר** או **היסט קיסר** או **הסטה קיסרית**, הוא אחד הצפנים הפשוטים והידועים בעולם ההצפנה.

זהו סוג של צופן החלפה שבו כל אות בטקסט מוחלפת על ידי אות הנמצאת בהיסט קבוע כלשהו ממנה באלף-בית. למשל אם נקבע את ההיסט להיות 3, האות A תוחלף באות D, האות B תוחלף באות E וכך הלאה.

הכינוי קיסר נובע מכך שיוליוס קיסר נהג להשתמש בצופן על מנת לתקשר עם מפקדיו.

צופן את-בש

כתב אתב"ש, הנקרא גם "**צופן אתב"ש**", הוא צופן החלפה. בצופן זה מוחלפות האותיות הראשונות בסדר האלפבית העברי באותיות האחרונות בו.

לפי כלל הא-ת ב-ש, אל"ף מוחלפת באות ת"ו, בי"ת מוחלפת באות שי"ן, גימ"ל מוחלפת באות רי"ש וכן הלאה. הרעיון הוא לחלק את עשרים ושתיים אותיות האלפבית העברי (לא כולל אותיות סופיות) לשני טורים מקבילים - האחד מתחיל מאל"ף והשני מתחיל מת"ו.

במקום כל אות במילה אותה מצפינים, כותבים את האות המקבילה בטור ההפוך.

לפיכך במקום המילה "שלום" נכתוב "בכפי". הפענוח נעשה בדרך זהה. בצופן החלפה, כאשר ידוע ההיסט, דהיינו הטבלה המתוארת, מלאכת הפענוח קלה מאוד. את ההיסט ניתן להשיג על ידי ניתוח תדירויות מופע של כל אות ואות. לרוב מספיק לפענח אות אחת (בתנאי שהמסר ארוך מספיק), בדר"כ זו בעלת תדירות ההופעה הגבוהה ביותר בשפה, ואז ניתן לחשב את ההיסט.

א	ת
ב	ש
ג	ר
ד	ק
ה	צ
ו	פ
ז	ע
ח	ס
ט	נ
י	מ
כ	ל
ל	כ
מ	י
נ	ט
ס	ח
ע	ז
פ	ו
צ	ה
ק	ד
ר	ג
ש	ב
ת	א

בס"ד

צופן ויז'נר

צופן ויז'נר הוא צופן החלפה רב-אלפביתי, המחליף כל אות במסר באות אחרת מתוך אלפבית שונה, קרי במפתח שונה.

השימוש במפתח נעשה באופן מחזורי. לאחר שימוש בכל האלפביתים חוזרים לאלפבית הראשון. מיקומה של כל אות במסר המקורי קובע באיזה אלפבית מתוך קבוצת האלפבית של מפתח הצופן להצפינה.

בכל מפתח אלפבית סדר האותיות שונה, כך שכל אות זהה במסר תוצפן לאות אחרת בצופן, על כן לא נשמרת תדירות האותיות שבמסר המקורי.

בניגוד לצופן חד-אלפביתי המבצע הזזה או החלפה של כל אותיות המסר במרחק קבוע.

חולשתו העיקרית - אורך המפתח.

אף על פי שצופן ויז'נר אינו משמר תדירות אותיות, מבחינה קריפטוגרפית אינו בטוח לשימוש, כיוון שהוא חשוף לניתוח סטטיסטי.

לפי תורת האינפורמציה, לכל שפה יתירות טבעית, כלומר אותיות המסר חוזרות על עצמן בתדירות שונה. יתירות מאפשרת ניתוח סטטיסטי של הצופן בהתאם לכללי היתירות של השפה הספציפית, למשל, האות "י" בשפה העברית אמורה לחזור על עצמה בתדירות גבוהה יותר מאשר האות "פ". ניתן להכין טבלת שכיחויות של אותיות האלפבית לשפה הנתונה, מתוך כמות נכבדה של טקסט רגיל ולפי זה לבצע ניתוח של הצופן

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

בס"ד

אניגמה

ה**אניגמה** (מיוונית: αἴνιγμα - תעלומה, חידה) היא משפחה של מכונות להצפנה ולפענוח של מסרים טקסטואליים, ששימשו את הכוחות הגרמנים והאיטלקים במלחמת העולם השנייה. בזכות התקשורת המוצפנת שאפשרה האניגמה, הצליח הקריגסמרינה (הצי הגרמני), ובמיוחד צי הצוללות, להטיל מצור אפקטיבי על בריטניה, מצור שמנע הובלת מזון ואמצעי לחימה לאי הבריטי.

בעלות הברית הצליחו לפצח את ההצפנה, ובמשך רוב המלחמה פענחו מספר גדול של הודעות מוצפנות. את המודיעין שנצבר מקריאת מסרי האניגמה כינו בשם "**אולטרה**". יש הטוענים כי אילולא פוצח צופן האניגמה, היה המצור הימי על בריטניה עלול להמיט אסון על תושבי האי. פיצוח הצופן הקנה לצי הבריטי יתרון משמעותי במלחמה מול חיל הים הגרמני, והיכולת, שהייתה יתרון אסטרטגי משמעותי, נשמרה בסוד במשך עשרות שנים.